Quantum Key Distribution Highly Sensitive to Eavesdropping

Stephen Brierley
Department of Mathematics, University of York
Heslington, York, UK YO10 5DD
sb572@york.ac.uk

October 2009

Abstract

We introduce a new quantum key distribution protocol that uses d-level quantum systems to encode an alphabet with c letters. It has the property that the error rate introduced by an intercept-and-resend attack tends to one as the numbers c and d increase. In dimension $d = 2$, when the legitimate parties use a complete set of three mutually unbiased bases, the protocol achieves a quantum bit error rate of 57.1%. This represents a significant improvement over the 25% quantum bit error rate achieved in the BB84 protocol or 33% in the six-state protocol.

1 Introduction

By sharing a random string of numbers, two parties can encrypt a message in such a way that it appears completely random to an eavesdropper. The "one-time pad" is an unbreakable method of encryption provided the string is truly random and only used once. The problem comes in having sufficiently many strings, called keys, with which to encrypt all messages you wish to send. This is called the key distribution problem.

By allowing the security of the key distribution protocol to be *computationally* impossible rather than unconditional, several ingenious methods to distribute keys have been developed. Assuming that an eavesdropper does not posses an infinitely large computer, cryptographic systems can make use of mathematical problems that are very hard to solve. For example, there is no known efficient algorithm to factorize large integers into a product of primes (used in the Rivest-Shamir-Adleman algorithm [1]) or to compute the discrete logarithm (used in the Diffe-Hellman-Merkle key exchange [2, 3]). However, solving these mathematical problems is only difficult, not impossible, so that the security of such public key protocols relies on the lack of future developments in mathematics and technology.

In 1970, Wiesner proposed a totally new approach to cryptography [4] that was then developed by Bennett and Brassard: they presented a key distribution protocol [5], now known as BB84, that uses properties of quantum systems to ensure its security. This protocol allows two parties, Alice and Bob, to distribute a key such that anyone who attempts to listen in on the quantum signals can, in theory, be detected. The eavesdropper, Eve, is constrained by the physical laws of quantum mechanics. She cannot perform a measurement without introducing a disturbance (Heisenberg's uncertainty principle), copy

states (no cloning) or split the signal, since it consists of single photons or particles. Other protocols such as Ekert's [6] use entangled particles in such a way that Eve essentially introduces hidden variables destroying the quantum correlations. It is possible to prove that these quantum key distribution (QKD) protocols are secure against all future technological and mathematical advances[1] [8, 9].

When attempting to implement a QKD protocol a key factor in determining its *practical* success is the error rate introduced by Eve: if it is small, her presence may be masked by the system noise. This error rate thus determines the level of technology required to implement the protocol and the distance over which Alice and Bob can establish a secure key. We will present a protocol that extends the one proposed by Khan et al. [10]. The new approach ensures that eavesdropping causes a large error rate and therefore, from an experimental point of view, offers a modification that could improve the implementation of existing QKD technology.

The new protocol allows Alice and Bob a great deal of freedom: the elements of the key that they form can be taken from an alphabet of arbitrary size, and encoded using any bases of $\mathbb{C}^d$. It is equivalent to the protocol presented in [10] when Alice and Bob use a two-letter alphabet and corresponds to the SARG protocol [11] when in addition, they use two-dimensional quantum systems.

In order to better understand the freedom in the choice of bases used by all three parties, Alice, Bob and Eve, we will introduce a measure of distance between two bases and show how this relates to the error rate. It gives a simple interpretation of the optimal setup for all parties: Alice and Bob should use a set of c bases, $\mathcal{S}$, that are as far apart as possible; whilst Eve should choose her basis, $\mathcal{E}$, so it minimises the average distance between $\mathcal{E}$ and the elements of $\mathcal{S}$. The conclusion then is that for the legitimate parties, the optimal settings correspond to so called *mutually unbiased (MU) bases* or complementary observables. MU bases have the property that a measurement in any one of the bases reveals no information about the state in all of the other bases; and have been used before in other QKD protocols [5, 12, 13].

The paper is organised as follows. In Sec. 2, we will introduce a key distribution protocol that encodes a c-letter alphabet using quantum systems of dimension d. In Sec 3, we will examine the effect of an eavesdropper by calculating two error rates that allow the legitimate parties to detect Eve's intercept-and-resend attack. Sec. 4 will show how one of these error rates can be understood as a measure of the distance between the bases used by all three parties. We will consider some examples of specific sets of bases in Sec. 5. In Sec. 6, we compare this new protocol to the six-state protocol in an experimental setting and consider a general method of implementing the protocol for any choice of c and d. Finally, we summarise the results and compare the new protocol to existing quantum key distribution methods in Sec. 7.

2 General form of the Protocol

In quantum cryptography, there are two legitimate parties who wish to establish a shared sequence of letters from an alphabet such as a string of zeros and ones. Typically, these two parties have different roles: Alice prepares and sends quantum states, and Bob performs

[1] Except possibly a new theory of physics that allows operations beyond quantum mechanics (c.f. Popescu-Rohrlich boxes [7]).

measurements on the states he receives and records the outcomes. At the end of this quantum part of the protocol, the two parties then exchange information via a classical communication channel. A third party, Eve, attempts to gain information about some or all of the shared key without being detected. Eve can perform any operation allowed by quantum mechanics and can listen in on the classical part of the communication without being detected. We also assume that she has access to a high level of technology so that she can hide behind any system noise by replacing parts of the implementation by better components. The aim is to find protocols and implementations such that Eve is easily detected.

We begin by presenting a new protocol that enables Alice and Bob to share a key and then discuss the effect Eve has on the states received by Bob. We will assume that Eve uses an intercept-and-resend attack and calculate error rates that allow the legitimate parties to detect her presence. There are other more sophisticated forms of attack available to Eve but we will not analyse them here; we simply remark that this form of attack provides a useful guide to the security of the protocol against more general attacks.

We first present the *highly-sensitive-to-eavesdropping (HSE)* protocol in its general form; encoding an alphabet, $\mathcal{A}$, containing $c \equiv |\mathcal{A}|$ elements using d dimensional quantum systems. In Sec. 2.1, we give an explicit example of the protocol when used to encode a 4-letter alphabet, say $\{0, 1, 2, 3\}$, using 3-dimensional quantum systems. A further example is provided in Sec. 6.1 where we discus the case of $c = 3$ and $d = 2$ in an experimental setting.

The HSE-Protocol

- Alice and Bob agree publicly on a method of encoding the c elements of $\mathcal{A}$ using states in $\mathbb{C}^d$ by choosing bases $\mathcal{B}^x = \{|\psi_i^x\rangle \in \mathbb{C}^d : i = 1 \dots d\}$ for all $x \in \mathcal{A}$. They are free to choose any bases provided they are different in the sense that no two bases have any state in common. We will discuss the optimum choice in Sec. 4. Throughout the protocol, Alice and Bob will use bases chosen from the set $\{B^x : x \in \mathcal{A}\}$.

- Alice generates a random string, S, of letters from $\mathcal{A}$ that form the raw data she will attempt to share with Bob.

- For each element, $x \in S$, Alice generates $c-1$ random numbers, $\mathbf{a} \equiv (a_1, \dots a_{c-1})$, between 1 and d. The numbers $\mathbf{a}$ serve as indices for states chosen from basis $\mathcal{B}^x$ as she now prepares and sends the $c-1$ states $|\psi_{a_k}^x\rangle \in \mathcal{B}^x$, $k = 1 \dots c-1$, to Bob.

- Bob chooses a sequence of $c-1$ *different* letters of $\mathcal{A}$, $x_1, \dots, x_k$. When he receives the kth state, $|\psi_{a_k}^x\rangle$, he measures it in the bases $\mathcal{B}^{x_k}$ and records the measurement outcomes, $\mathbf{b} \equiv (b_1, \dots b_{c-1})$.

- After Bob's measurements, Alice publicly announces the indices $\mathbf{a}$ keeping her choice of basis a secret. Using this information, Bob is (sometimes) able to deduce which basis Alice used and therefore to determine the element of S.

- Bob tells Alice for which elements he was able to determine x. Unsuccessful attempts are discarded, leaving only the shared key.

An element $x \in S$ is successfully shared between Alice and Bob when for every state $|\psi_{a_k}^x\rangle \in \mathcal{B}^x$, $k = 1 \dots c-1$, the index measured by Bob does *not* equal the index announced

by Alice, $a_k \neq b_k$ for all k. If this happens Bob knows that *none* of his measurements were in basis $\mathcal{B}^x$ and so his missing basis corresponds to the correct letter of the string, x. If Bob's measurement does equal the announced index for any k, he does not know if this was because he measured in the same basis as Alice or because of the non-zero overlap between vectors from different bases. This element of the string then fails.

The protocol presented in [10] is then a special case of this protocol applied to a two-letter alphabet $\{0, 1\}$ so that Alice needs only to send one state for each letter of S. Khan et al.'s protocol is interesting because it has a high error rate that approaches 50% for higher dimensional quantum systems if Alice and Bob use two mutually unbiased bases. Starting with the probability that the transmission of the element x is successful, we will analyse the performance of the general protocol in the following sections. We find that this general protocol has an error rate that approaches 100% when Alice and Bob use high-dimensional systems and a complete set of $(d + 1)$ mutually unbiased bases. In Sec. 4 we will use a natural measure of distance between bases to argue that the optimal settings for Alice and Bob are indeed mutually unbiased bases.

2.1 A four-letter alphabet encoded using qutrits

We now make the protocol explicit when applied to a four-letter alphabet, say $\mathcal{A} = \{0, 1, 2, 3\}$, encoded using three-dimensional quantum systems. Note that we can think of $0, 1, 2, 3$ as representing 00, 01, 10, 11 and therefore the key that Alice and Bob share as pairs of bits, for example, the string $S = 213101$ becomes 100111010001; this makes it easier to compare the bit efficiency of different protocols. We examine the case where Alice and Bob encode $\mathcal{A}$ using the bases

$$\mathcal{B}^0 \simeq \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \mathcal{B}^1 \simeq \frac{1}{\sqrt{3}} \begin{pmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega \end{pmatrix},$$
$$\mathcal{B}^2 \simeq \frac{1}{\sqrt{3}} \begin{pmatrix} 1 & 1 & 1 \\ \omega^2 & 1 & \omega \\ \omega^2 & \omega & 1 \end{pmatrix}, \mathcal{B}^3 \simeq \frac{1}{\sqrt{3}} \begin{pmatrix} 1 & 1 & 1 \\ \omega & \omega^2 & 1 \\ \omega & 1 & \omega^2 \end{pmatrix}, \tag{1}$$

where the columns of the matrix $\mathcal{B}^x$ correspond to the vectors $|\psi_i^x\rangle, i = 1, 2, 3$ of each basis.

In order to send the first element of the string, say $x = 2$, Alice generates three random numbers $a_1, a_2, a_3 \in \{1, 2, 3\}$ and sends the states $|\psi_{a_1}^2\rangle$, $|\psi_{a_2}^2\rangle$ and $|\psi_{a_3}^2\rangle$. Bob now measures in three different, randomly chosen bases resulting in the measurement outcomes b_1, b_2 and b_3. The element x is successfully transmitted if and only if $a_1 \neq b_1$, $a_2 \neq b_2$ and $a_3 \neq b_3$ since if this happens, Bob can be certain that he did not use the same basis as Alice. Bob must have performed measurements in the bases $\mathcal{B}^0$, $\mathcal{B}^1$ and $\mathcal{B}^3$ so that his missing basis corresponds to the correct element $x = 2$. The probability that an element is shared for each run of the protocol is given by

$$\mathcal{R}_s \equiv \frac{1}{4}\left(1 - \frac{1}{3}\right)^3 = \frac{2}{27},$$

since there is a 1/4 chance that Bob does *not* use $\mathcal{B}^2$ and a 2/3 chance that he does *not* measure index a_k when using basis $\mathcal{B}^x$, $x \neq 2$, for $k = 1 \ldots 3$.

Each element of the string represents two bits and so, on average, in order to share one

bit of information Alice and Bob need to perform this procedure $27/4 \approx 7$ times so that Alice has to send a total of $3 \times 27/4 \approx 20.3$ states. This is relatively high, for example in the BB84 protocol, Alice needs to send an average of only two states in order to successfully transmit one bit of information. However, as we will see in Sec 3, the presence of an eavesdropper causes a much higher error rate. The present protocol therefore remains secure even if there is a very high level of system noise.

2.2 Probability of success

Having calculated the success rate for the protocol in the case of a four-letter alphabet encoded using a specific choice of bases of $\mathbb{C}^3$, we now consider the general probability of success. The protocol results in a letter, x, forming part of the shared key whenever the indices measured by Bob are all different from those announced by Alice, that is whenever $a_k \neq b_k$ for $k = 1, \ldots, c-1$. For each state, indexed by k, Bob makes a measurement in basis B^{x_k} so that the probability of measuring index a_k is given by

$$q_k \equiv \text{prob}(a_k = b_k) = \left| \langle \psi_{a_k}^{x_k} | \psi_{a_k}^{x} \rangle \right|^2 .$$

Hence the success rate of the protocol is

$$\mathcal{R}_s \equiv \frac{1}{c} \prod_{k=1}^{c-1} (1 - q_k), \tag{2}$$

the chance that none of the $c-1$ bases chosen by Bob equal the one selected by Alice, $\mathcal{B}^x$, multiplied by the probability of never measuring the same index even though all of Bob's measurements are different to $\mathcal{B}^x$. In order to get a success rate *per bit* of information shared between Alice and Bob, called the *bit transmission rate,*

$$\mathcal{R}_t \equiv \log_2(c) \mathcal{R}_s, \tag{3}$$

we multiply $\mathcal{R}_s$ by $\log_2(c)$.

This general formula depends on the choice of bases used to encode the alphabet, and in particular the modulus of the overlap between states from different bases. We will consider different bases used in the protocol in Sec. 5 and compare the bit transmission rate, $\mathcal{R}_t$, with existing QKD protocols in the conclusion.

3 Error rate introduced by an eavesdropper

We have seen how the protocol allows Alice and Bob to create a shared key, we now consider the effect of an eavesdropper. In particular, we analyse the effect of an intercept-and-resend attack. That is, for each state sent by Alice, an eavesdropper performs a measurement on the system and then prepares and sends a new state to Bob. In effect, we can imagine the attack as being performed in two stages. Eve measures the state of the system and then discards it completely. Using the classical information corresponding to her measurement outcome, she then prepares a new system in a state that is as "close as possible" to the original.

In general, Eve is free to use different measurements for each state sent by Alice. She can also send Bob a system in any state regardless of the measurement outcome. However, since

the states $|\psi^x_{a_k}\rangle$ have indices, a_k, that are uniformly distributed, each subsequent measurement made by Eve is independent from the previous measurement outcomes. Therefore, there is no loss of generality in assuming that Eve always uses the same measurement basis, $\mathcal{E} = \{|e_i\rangle \in \mathbb{C}^d, i = 1 \ldots d\}$, corresponding to her optimal one. In addition, we assume that Eve sends the state corresponding to her measurement outcome since it is likely to be the state closest to $|\psi^x_{a_k}\rangle$.

Alice and Bob can detect Eve's attack in one of two different ways; by detecting a change in the index of the state received by Bob, called the *index transmission error rate* (ITER); and by errors in the final shared key, called the *quantum bit error rate* (QBER). We begin by considering the ITER, which can be detected whenever Alice and Bob use the *same* bases, $\mathcal{B}^x$, and has been used in other QKD protocols to detect an eavesdropper [10, 14, 15].

3.1 The index transmission error rate

Suppose Alice sends the state $|\psi^x_i\rangle$, Bob can detect Eve if he happens to perform a measurement in basis $\mathcal{B}^x$ and his measurement outcome, j, does not equal i. This occurs with probability $p_i(x,x)$, where we define

$$p_i(x,y) \equiv \sum_{k=1}^{d} \sum_{\substack{j=1 \\ j\neq i}}^{d} |\langle\psi^x_i|e_k\rangle|^2 |\langle e_k|\psi^y_j\rangle|^2, \tag{4}$$

to be the probability that the index i changes when Alice prepares a state in basis $\mathcal{B}^x$ and Bob measures the system he receives in basis $\mathcal{B}^y$. Since for any y and k, Eve measures one of the possible outcomes with certainty,

$$\sum_{j=1}^{d} |\langle e_k|\psi^y_j\rangle|^2 = 1, \tag{5}$$

Eqn. (4) can be written as

$$p_i(x,y) = 1 - \sum_{k=1}^{d} |\langle\psi^x_i|e_k\rangle|^2 |\langle e_k|\psi^y_i\rangle|^2,$$

one minus the probability that Bob measures a state with index i.

The rate at which Alice and Bob can detect an index transmission error, $\mathcal{R}_{IT}$, is calculated by averaging $p_i(x,x)$ over all indices, i, and letters of the alphabet, $x \in \mathcal{A}$. That is,

$$\begin{aligned} \mathcal{R}_{IT} &\equiv \frac{1}{cd} \sum_{x=0}^{c-1} \sum_{i=1}^{d} p_i(x,x) \\ &= 1 - \frac{1}{cd} \sum_{x=0}^{c-1} \sum_{i=1}^{d} \sum_{k=1}^{d} |\langle\psi^x_i|e_k\rangle|^4. \end{aligned} \tag{6}$$

As with the probability of success, $\mathcal{R}_{IT}$ depends on the choice of bases. We will see how

this measure of the sensitivity of the protocol to eavesdropping can be understood as a measure of distance between the bases used by all three parties in Sec. 4. Then in Sec. 5 we will consider some interesting examples of specific bases.

3.2 The quantum bit error rate

In addition to the index transmission error rate, Alice and Bob can detect an eavesdropper by calculating the error rate of the final shared key. Eve's intercept-and-resend attack may cause a change in the index in such a way that Bob adds an incorrect letter to his key. Just as in the original BB84 protocol, the legitimate parties can detect quantum bit errors by selecting a random subset of the key and openly comparing its elements.

To see how an error in the key is created, suppose Alice attempts to share the letter $x \in \mathcal{A}$. If none of the indices measured by Bob equal the indices announced by Alice, $a_k \neq b_k$ for all $k = 1 \dots c-1$, Alice adds x to her key and Bob adds $\widetilde{x}$. The letters, x and $\widetilde{x}$, correctly coincide provided one of Bob's measurements was not in the basis $\mathcal{B}^x$ since he adds the letter corresponding to his missing basis. If however, Bob did use $\mathcal{B}^x$, he adds the letter $\widetilde{x} \neq x$ to his key and there is an error in the shared key. Therefore, the proportion of key elements that contain an error, is given by the *quantum bit error rate*

$$\mathcal{R}_{QB} \equiv \frac{c-1}{c} \frac{\mathcal{R}_{BE}}{\mathcal{R}_K}, \tag{7}$$

where; the factor $\frac{c-1}{c}$ is the probability that Bob uses the same basis as Alice in one of his $c-1$ measurements; $\mathcal{R}_{BE}$ is the rate at which Bob adds incorrect letters to his key, called *Bob's error rate*; and $\mathcal{R}_K$ is the average probability that a bit is added to the key regardless of Bob's choice of basis, called the *key rate*.

We now calculate the terms in Eqn. (7) starting with $\mathcal{R}_K$. Given any vector of indices, $\mathbf{a} = (a_1, \dots, a_{c-1})$, chosen by Alice and bases with indices $\mathbf{y} = (y_1, \dots, y_{c-1})$ chosen by Bob, the probability that $a_k \neq b_k$ for all $k = 1 \dots c-1$ is given by

$$\prod_{k=1}^{c-1} p_{a_k}(x, y_k). \tag{8}$$

where $p_i(x, y)$ has been defined in Eqn. (4). Alice uses vectors from the set $I \equiv \{(a_1, \dots, a_{c-1}) : a_k \in \mathbb{Z}_d\}$ since she is free to repeat an index. Bob, however is more restricted, he must use each basis only once and therefore, choose a vector

$$\mathbf{y} \in Y \equiv \{(y_1, \dots, y_{c-1}) : y_k \in \mathcal{A} \text{ and } y_k \neq y_l \text{ for all } k, l\}.$$

Hence, $\mathcal{R}_K$ is the average over all bases $\mathcal{B}^x$ and elements of the sets I and Y,

$$\mathcal{R}_K = \frac{1}{c|Y||I|} \sum_{x=0}^{c-1} \sum_{\mathbf{y} \in Y} \sum_{\mathbf{a} \in I} \prod_{k=1}^{c-1} p_{a_k}(x, y_k), \tag{9}$$

where $|Y| = c!$ and $|I| = d^{c-1}$.

The numerator in Eqn. (7), $\mathcal{R}_{BE}$, is the average probability that Bob adds an incorrect letter to his key. Such a bit error occurs when Bob uses the same basis as Alice *and* measures indices that are all different to those announced by Alice. To help calculate Bob's error

rate, we define the set Z to be

$$Z \equiv \{(x, z_2, \ldots, z_{c-1}) : z_k \in \mathcal{A},\, z_k \neq x \text{ and } z_k \neq z_l \text{ for all } k, l\},$$

that is, the first component of every $\mathbf{z} \in Z$ corresponds to the letter x used by Alice to encode the states. Therefore, Bob's error rate is given by

$$\mathcal{R}_{BE} = \frac{1}{c|Z||I|} \sum_{x=0}^{c-1} \sum_{\mathbf{z}\in Z} \sum_{\mathbf{a}\in I} \prod_{k=1}^{c-1} p_{a_k}(x, z_k), \tag{10}$$

where we average over all outcomes that correspond to Bob adding an incorrect letter to his key and the set Z contains $|Z| = (c-1)!$ elements.

The rather complicated formula for $\mathcal{R}_{QB}$ given by Eqns. (7), (9) and (10) has a simple form when Alice and Bob use only two bases in the protocol. The simplification is due to the fact that when $c = 2$, Bob's error rate $\mathcal{R}_{BE} = \mathcal{R}_{IT}$ and hence

$$\mathcal{R}_{QB} = \frac{\mathcal{R}_{IT}}{2\mathcal{R}_K} \quad \text{for } c = 2,$$

corresponding to the QBER obtained in [10]. We will also see that the general form of $\mathcal{R}_{QB}$ simplifies when applied to a specific choice of bases in Sec. 5. Before doing so, we show how the error rate $\mathcal{R}_{IT}$ relates to a natural measure of distance between the bases of $\mathbb{C}^d$ used by the three parties.

4 Distance between bases

In this section we consider the bases used in the QKD protocol as points in a higher-dimensional space. This setting allows us to understand the optimal strategy for the legitimate parties in terms of a natural measure of distance between two bases. We follow an approach similar to that presented in [16]; here, however, we will consider an alternative choice of origin so that the resulting space is an *affine* space rather than a vector space.

We begin by associating to every normalised vector, $|\psi\rangle \in \mathbb{C}^d$, the operator

$$|\psi\rangle \rightarrow \psi = |\psi\rangle\langle\psi|$$

that lives in a $d^2 - 1$ dimensional space consisting of Hermitian operators of trace one. Equipped with the inner product

$$\psi \cdot \phi = \mathrm{Tr}\psi\phi,$$

this is an affine space in which a basis $\mathcal{B} = \{|\psi_1\rangle, |\psi_2\rangle, \ldots, |\psi_d\rangle\}$ of $\mathbb{C}^d$ is identified with a set of operators $\{\psi_1, \psi_2, \ldots, \psi_d\}$ spanning a $d-1$ dimensional plane. To define a distance between two such planes, we perform a similar procedure and embed them in an even larger space so that to each basis $\mathcal{B}$ we associate the matrix

$$\Psi = \frac{1}{\sqrt{d}} [\psi_1 \psi_2 \ldots \psi_d] \begin{bmatrix} \psi_1^T \\ \psi_2^T \\ \vdots \\ \psi_d^T \end{bmatrix},$$

that projects onto the plane spanned by the basis vectors $\{\psi_1, \psi_2, \ldots \psi_d\}$. Acting on an arbitrary pure state, ϕ, the operator Ψ describes the action of performing a measurement in basis $\mathcal{B}$ since the non-zero elements of $\Psi\phi$ are $|\langle\psi_i|\phi\rangle|^2\, \psi_i$ for $i = 1 \ldots d$.

The matrices Ψ are elements of a $(d^2-1)^2$ dimensional space (called an affine Grassmannian), in which a natural measure of distance between two points, Φ and Ψ, is the chordal Grassmannian distance

$$D^2(\Phi, \Psi) = 1 - \mathrm{Tr}\Phi\Psi. \tag{11}$$

Applying this distance measure to two points, Φ and Ψ, associated with bases reads

$$\begin{aligned} D^2(\Phi,\Psi) &= 1 - \frac{1}{d}\mathrm{Tr}\left\{ [\psi_1\psi_2 \ldots \psi_d] \begin{bmatrix} \psi_1^T \\ \psi_2^T \\ \vdots \\ \psi_d^T \end{bmatrix} [\varphi_1\varphi_2 \ldots \varphi_d] \begin{bmatrix} \varphi_1^T \\ \varphi_2^T \\ \vdots \\ \varphi_d^T \end{bmatrix} \right\} \\ &= 1 - \frac{1}{d}\sum_{i=1}^{d}\sum_{j=1}^{d}(\psi_i \cdot \varphi_j)^2 \\ &= 1 - \frac{1}{d}\sum_{i=1}^{d}\sum_{j=1}^{d}|\langle\psi_i|\varphi_j\rangle|^4\,. \end{aligned}$$

Hence the average distance, $D_{average}$, between Eve's basis E and the bases chosen by Alice and Bob, B^x, $x = 0 \ldots c-1$, is given by

$$\begin{aligned} D_{average} &= \frac{1}{c}\sum_{x=0}^{c-1} D^2(B^x, E) \\ &= 1 - \frac{1}{cd}\sum_{x=0}^{c-1}\sum_{i=1}^{d}\sum_{k=1}^{d}|\langle e_k|\psi_j^x\rangle|^4 \\ &= \mathcal{R}_{IT}, \end{aligned} \tag{12}$$

the index transmission error rate caused by Eve's intercept-and-resend attack.

This distance measure provides an intuitive feel as to how the three parties in the protocol should behave: Alice and Bob aim to maximize the error rate $\mathcal{R}_{IT}$ by separating their bases as much as possible; whilst Eve chooses a basis that minimises the average distance between all of the bases chosen by Alice and Bob. We will begin the next section by making these statements more precise and find that they lead to the conclusion that Alice and Bob should use a complete set of mutually unbiased bases.

5 Optimal choice of bases

In this section we consider specific choices of bases used by Alice and Bob in the HSE-protocol. The protocol is entirely general and any set of bases can be used to encode the alphabet. There are likely to be many considerations in choosing a suitable set such as the ease of preparing and measuring states in each of the prescribed bases. In this section we will not worry about experimental difficulties but simply consider the optimal choice

from a theoretical perspective. Motivated by the distance measure in Sec. 4 we begin by considering a set of mutually unbiased (MU) bases.

5.1 Mutually unbiased bases

Two bases $\mathcal{B}^x = \{|\psi_i^x\rangle, i = 1 \dots d\}$ and $\mathcal{B}^y = \{|\psi_i^y\rangle, i = 1 \dots d\}$ are called mutually unbiased if the modulus of the inner product of vectors from different bases is uniform,

$$|\langle\psi_i^x|\psi_j^y\rangle| = \kappa, \tag{13}$$

which in finite dimensions means that $\kappa = 1/\sqrt{d}$. Schwinger noted [17] that two such bases represent measurements that are "maximally non-commuting" in that measuring in one bases reveals no information about the outcome of a measurement in the other basis. For example, in dimension $d = 2$, if we set a Stern-Gerlach experiment to measure spin in the x direction, we gain no information about spin in the z direction.

This maximal lack of information about measurement outcomes from other bases is captured by the distance measure introduced in Eqn. (11). The distance between any two bases Φ and Ψ, is bounded by

$$0 \leq D^2(\Phi, \Psi) \leq 1 - \frac{1}{d},$$

where the lower bound is obtained when Φ and Ψ span the same subspace and the upper bound is realised when they are mutually unbiased. Since Alice and Bob wish to maximize the average distance between all of the bases they use, a natural strategy is to use as many MU bases as possible. They cannot use more than $d+1$, called a *complete set*, since it is impossible to fit any more $d-1$ dimensional planes with the correct overlap into a space of dimension d^2+1 [16]. In dimension $d = 3$, the four bases given in Eqn (1) constitute a complete set of MU bases. In all other prime-power dimensions, a complete set of MU bases has been constructed [18]. However, for composite dimensions $d = 6, 10, 12, ...$ the maximum number of bases satisfying the conditions (13), remains an open problem.

We now turn our attention to the optimal strategy of an eavesdropper. As before, we assume that she uses an intercept-and-resend attack and following the arguments of Sec. 3, only uses one basis corresponding to her optimal choice. Eve's optimal strategy is essentially a minimisation problem subject to some constraints. The functions she wishes to minimise are the error rates $\mathcal{R}_{QB}$ and $\mathcal{R}_{IT}$, and the constraints come from the fact that Eve must use a set of d orthonormal vectors. By approaching this problem numerically, Khan et. al. provide evidence that for $c = 2$, the index transmission error rate has a global minimum when Eve's basis spans the same subspace as one of the bases chosen by Alice and Bob [10]. In other words, Eve's optimal strategy is to simply pick one of the bases used by the legitimate parties.

Eve has many alternative eavesdropping strategies at her disposal. For example, for the case when $d = c = 2$, Eve could use the so-called Breidbart basis that is halfway between the two bases used by the legitimate parties [19]. In the BB84 protocol, such a strategy has been shown to increase the chance that Eve reads the bit correctly although it does not reduce her chance of being detected [20]. However, when the legitimate parties use a complete set of MU bases, there is no basis that is "halfway" between all of them. There are many issues concerned with finding the optimal strategy of an eavesdropper

[21, 22, 23, 24]. In the following, we will assume that Eve picks one of the bases used by the legitimate parties and consider the protocol when Alice and Bob use a set of c MU bases.

There is no loss of generality in assuming that Eve's basis is given by $\mathcal{E} \equiv \{|e_i\rangle \in \mathbb{C}^d, i = 1 \ldots d\} = \mathcal{B}^0$. Under this assumption, the distance between the bases used by all three parties is

$$D^2(E, B^x) = \begin{cases} 0 & \text{if } x = 0 \\ 1 - \frac{1}{d} & \text{if } x \neq 0, \end{cases}$$

zero if $\mathcal{B}^x$ corresponds to $\mathcal{E}$ or maximal otherwise. Hence, the index transmission error rate for a set of c MU bases is given by

$$\begin{aligned} \mathcal{R}_{IT}^{MUB} &= \frac{1}{c} \sum_{x=1}^{c-1} \left(1 - \frac{1}{d}\right) \\ &= \frac{(c-1)(d-1)}{cd}. \end{aligned} \tag{14}$$

We see that the error rate is an increasing function of both c and d and that Eqn. (14) is indeed maximized if Alice and Bob use a complete set of MU bases. In which case, the index transmission error rate of the protocol equals

$$\mathcal{R}_{IT}^{MUB} = \frac{d-1}{d+1}$$

and therefore tends to 100% as d tends to infinity.

The index transmission error rate introduced by an intercept-and-resend attack in Eqn. (14) is equal to the quantum bit error rate of the BKB01-protocol of Bourennane et al. [12]. It is a natural generalisation of the BB84 protocol and has been further analysed in [25, 13]. The BKB01-protocol, the d letters of an alphabet are encoded into the indices of one of c mutually unbiased bases. Alice sends a state $|\psi_x^a\rangle$, where $x = 1 \ldots d$ and $a = 0 \ldots c-1$, and after Bob's measurement, announces the basis, a, which she used to prepare the states. Hence, whenever Bob performs a measurement in the same basis $\mathcal{B}^b$, they share the letter $x \in \mathcal{A}$. Note that in contrast to the HSE-protocol, the roles of c and d are reversed. In the conclusion, the error rates and the number of states needed to successfully share one bit of the key for the BKB01 protocol are compared to the HSE-protocol.

The quantum bit error rate, $\mathcal{R}_{QB}$, given in Eqn. (7), also simplifies significantly when Alice and Bob use a set of c MU bases and we assume that Eve's basis equals $\mathcal{E} = \mathcal{B}^0$, say. Under these assumptions, the probability that an index changes is zero if all three parties use the same bases and one minus the probability of measuring the correct index if any one of the parties uses a different basis

$$p_i(x, y) = \begin{cases} 0 & \text{if } (x, y) = (0, 0) \\ 1 - \frac{1}{d} & \text{if } (x, y) \neq (0, 0). \end{cases}$$

Therefore, the product of probabilities given in Eqn. (8),

$$\prod_{k=1}^{c-1} p_{a_k}(x, y_k),$$

depends solely on whether any of the terms correspond to $(x, y_k) = (0, 0)$.

To calculate the number of non-zero terms in $\mathcal{R}_{BE}$, given in Eqn. (10), note that one of Bob's bases is always equal to $\mathcal{B}^x$ and therefore $(x, y_k) = (0, 0)$ for some k, if and only if $x = 0$. Hence, the proportion of non-zero terms in Eqn. (10) is equal to $(1 - 1/c)$. Similarly, when the vectors $\mathbf{y} \in Y$, the number of non-zero terms in Eqn. (9) is $\left(1 - \frac{1}{c} + \frac{1}{c^2}\right)|Y||I|c$, so that Bob's error rate and the key rate are given by

$$\begin{aligned}\mathcal{R}_{BE} &= \left(1 - \frac{1}{c}\right)\left(1 - \frac{1}{d}\right)^{c-1} \\ \mathcal{R}_{K} &= \left(1 - \frac{1}{c} + \frac{1}{c^2}\right)\left(1 - \frac{1}{d}\right)^{c-1},\end{aligned}$$

respectively. Therefore, for a set of c mutually unbiased bases, the error rate $\mathcal{R}_{QB}$ is given by

$$\mathcal{R}_{QB}^{MUB} = \left(1 - \frac{1}{c}\right)^2 \left(1 - \frac{1}{c} + \frac{1}{c^2}\right)^{-1} \tag{15}$$

which, surprisingly, does *not* depend on the dimension of the quantum systems used in the protocol. However, it is of course limited by the number of MU bases that can be constructed in a given dimension $c \leq d + 1$ and may also be limited by the conjectured non-existence of complete sets of MU bases in composite dimensions.

Whilst constructions of complete sets of MU bases are known for prime power dimensions, and are well understood in low dimensions [26] their existence is an open problem for composite dimensions. In fact, there is considerable numerical [27, 28] and analytical [29, 30] evidence to suggest that there are no more than three MU bases in dimension six. Hence restricting the measurements to MU bases could mean that the protocol is more efficient in prime power dimensions than in composite dimensions, for example, using six MU bases in dimension five the error rate $\mathcal{R}_{IT}$ is $2/3 \approx 66.7\%$ were as if only three MU bases are available in dimension six the maximum error rate is $5/9 \approx 55.6\%$. The situation for the QBER is even more pronounced since $\mathcal{R}_{QB}^{MUB}$ depends only on the number of MU bases available and not on the dimension. As such it would be better to use quantum systems of dimension three since it is possible to construct four MU bases than to use systems of dimension $d = 6$, for which we only know how to construct three bases with the required overlap.

5.2 Approximate mutually unbiased bases

It is not clear that a complete set of $d+1$ mutually unbiased bases exists in all dimensions. Therefore, in order to consider the limiting behaviour of the protocol, we consider an alternative choice of bases for which constructions are known in all dimensions. As with a complete set of MU bases, they have the property that the error rate $\mathcal{R}_{IT}$ tends to 100% as the dimension of the quantum systems used by Alice and Bob increases.

By relaxing the uniform modulus condition (13), Klappenecker et al. [31] define approximate mutually unbiased bases (abbreviated as AMU bases) which have the property that the modulus of the inner product between vectors from different bases is small. In

particular they define a set of d^2 bases such that

$$|\langle\psi_i^x|\psi_j^y\rangle| \leq \frac{2+O(d^{-1/10})}{\sqrt{d}} \quad \text{for } x \neq y,$$

and for all i, j, where $f(d) = O(d^{-1/10})$ means that there exists a constant $K > 0$ such that $|f(d)| \leq Kd^{-1/10}$ for all $d \geq 1$. Hence if Alice and Bob use all d^2 bases, and Eve uses one of the bases in her intercept-and-resend attack, the index transmission error rate is bounded from below by

$$\mathcal{R}_{IT}^{AMUB} \geq 1 - \frac{1}{d^3}\left[d + (d^2-1)(2+Kd^{-1/10})^4\right]. \tag{16}$$

The unknown constant in Eqn. (16) prevents us from saying anything in specific dimensions, but we can still consider the protocol when Alice and Bob use a set of AMU bases in the limit as d tends to infinity. We see that such a set of approximate MU bases defined so that they minimise the value of κ in Eqn. (13) and therefore maximise the distance measure defined by Eqn. (12) are good at detecting the eavesdropping by Eve. Even though a complete set of MU bases may not exist in every dimension, we can at least define a set of AMU bases that do exist in all dimensions and for which the ITER tends to 100%.

6 Implementations

In this section, we present a specific example of how Alice and Bob can use the HSE-protocol to form a shared key. We also calculate the quantum bit and index transmission error rates that allow Alice and Bob to detect an eavesdropper for this choice of c and d. Finally, we discuss a practical implementation of the protocol that could be used for any values of c and d using photon states and multiport beam splitters.

6.1 An alternative "six-state" protocol using qubits

In the six-state protocol [24, 32], Alice prepares and sends one of six states corresponding to the points on the Bloch ball $(\pm1, 0, 0)$, $(0, \pm1, 0)$ and $(0, 0, \pm1)$. These six states form three MU bases $\mathcal{B}^0$, $\mathcal{B}^1$, and $\mathcal{B}^2$ corresponding to

$$\{|0\rangle, |1\rangle\}, \{\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\}, \text{ and } \{\frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle), \frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle)\}$$

respectively. After receiving a state from Alice, Bob performs a measurement in one of the three bases and records his outcome. Alice announces which of the bases she used to prepare the state and if Bob used the *same* basis they are able to share an element of the key. When the bases used by Alice and Bob coincide, Bob can correctly determine the letter because his measurement outcome must correspond to the state prepared by Alice (in the absence of an eavesdropper).

Using the polarization of photons to encode the states, Enzer et. al. have implemented the six-state protocol experimentally [33]. The three bases in their scheme correspond to horizontal/vertical (H/V), diagonal +45°/−45° (D/d) and left/right circular (L/R) polarization; the three states H,D and L encoding a zero and V,d,R a one. By simulating an

intercept-and-resend attack Enzer et. al. find a bit error rate of $34.0 \pm 1.4\%$ in agreement with the theoretical value of 33.3%.

In order to implement the HSE-protocol, the six-state scheme presented in [33] requires only a slight modification. The preparation and measurement of the states remains the same; the difference being the method of encoding the alphabet. Here, we will use the polarizations H/V to encode a zero, D/d a one and L/R a two. That is, our scheme uses a three letter alphabet $\mathcal{A} = \{0, 1, 2\}$ encoded into the choice of basis; $\mathcal{B}^0$, $\mathcal{B}^1$, or $\mathcal{B}^2$. The indices of the states are either zero or one corresponding to H,D, and L or V,d and R respectively.

As before, Alice chooses one of the bases $\mathcal{B}^0$, $\mathcal{B}^1$, or $\mathcal{B}^2$ but this time sends *two* states. That is, suppose Alice chooses to encode the bits in the H/V basis, then she sends either HH, HV, VH or VV. Bob now makes a measurement in two *different* bases and records the indices corresponding to his outcomes. Alice announces the indices, either 00, 01, 10 or 11, equal to her choice of prepared states. She does not announce the basis. Using the indices announced by Alice and his measurement outcomes, Bob hopes to determine the basis used by Alice.

An element of the key is shared whenever Bob's indices both differ from the indices announced by Alice. For example, if Alice sends states with indices 01, an element of the key is shared if and only if Bob's measurement outcomes are 10. For this scheme, the average rate at which a bits are shared between Alice and Bob is given by

$$\mathcal{R}_t = \log_2(3)\frac{1}{3}\left(1 - \frac{1}{2}\right)^2 \approx 13.2\%,$$

since the probability that Bob does not use the same basis as Alice in both of his measurements is 1/3 and there is a 1/2 chance that he does not measure the announced index when using a different basis. The pre-factor of $\log_2(3)$ is due to the fact that when an element of the key is shared it corresponds to an element of of a *three* letter alphabet.

Whilst the bit rate is 13.2%, compared to 33% for the six-state protocol, the number of sates Alice must send in order to share one bit of information is much higher than in the six-state protocol. For each attempt at sharing a letter of the alphabet, Alice must send two states. Therefore the average number of states, $\mathcal{N}_s = 2 \times 100/13.2 \approx 15.2$ which is five times more than the 3 states needed to share one bit when implementing the six-state protocol.

We find that although this protocol is more expensive than the six-state protocol, it is also more sensitive to an eavesdropper. The quantum bit error rate of an intercept-and-resend attack of this new protocol is given by

$$\mathcal{R}_{QB}^{MUB} = \left(1 - \frac{1}{3}\right)^2 \left(1 - \frac{1}{3} + \frac{1}{3^2}\right)^{-1} = \frac{4}{7} \approx 57.1\%,$$

following Eqn. (15); representing a significant improvement over the 33.3% error rate of the six-state protocol. We have used the *same* six states as the six-state protocol but this new method of encoding the letters of an alphabet is more sensitive to an intercept-and-resend attack.

6.2 Possible implementation using multiport beam splitters

A recent experiment has implemented quantum state tomography using a complete set of MU bases in dimension $d = 4$ [34]. It demonstrates that tomography with MU bases is not only optimal in theory, but is more efficient than standard measurement strategies in practice. The scheme presented in [34] therefore provides a way of measuring two-qubit photon states in one of five mutually unbiased bases in dimension four. However, to implement the QKD presented in Sec. 2 a set of c MU bases, we also need to reliably *prepare* the relevant states. Such a scheme for $c = 2$ MU bases has been provided by Khan et al. [10] and can be extended to any number of mutually unbiased bases. This follows from the fact that *any* discrete unitary operator can be realised using a series of beam splitters and mirrors [35]. These so called *multiport beam splitters* are symmetric when they correspond to MU bases [36].

The protocol could be implemented as follows. Alice uses a single photon source such as a spontaneous parametric down conversion crystal. She now chooses one of $c-1$ multiport beam splitters, or to bypass the beam splitters altogether. This gives one of the c bases labeled by the letters of $\mathcal{A}$ required for the protocol. Each vector $|\psi_i^x\rangle$ of her chosen basis, $\mathcal{B}^x$, is encoded into the output paths of the corresponding beam splitter by sending a single photon into the input port i. Bob uses the same beam splitters in order to measure the state of each photon he receives. He does this by first sending it through one of the beam splitters (or bypasses them to measure $\mathcal{B}^0$) and then detecting it in one of the d output ports. When $c = 2$, a natural choice for the two MU bases is to use the standard basis $\mathcal{B}^0 = \{|i\rangle, i = 0 \dots d-1\}$ and the so called Fourier matrix which has entries $F_{ij} = \omega^{ij}/\sqrt{d}$, for $i, j = 0 \dots d-1$ where $\omega = \exp(2\pi i/d)$ is the dth root of unity (which for $d = 3$ is given by $\mathcal{B}^1$ in Eqn. (1)). This scheme corresponds to the one presented in [10] and could be realised using Bell multiport beam splitters [37].

7 Conclusion

We have presented a novel protocol that enables two parties to generate a shared key. It is special in that the presence of an eavesdropper who uses an intercept-and-resend attack creates a *high error rate*. This has the practical advantage of allowing Alice and Bob to detect Eve even if the system noise in their implementation is high. We have analysed two error rates that allow for the detection of an eavesdropper; the *index transmission error rate* (ITER) and the *quantum bit error rate* (QBER). Both of these measures of the sensitivity to eavesdropping tend to one as the parties use more bases to encode the elements of the key and, in the case of the ITER, if they use higher dimensional systems.

Table 1 compares the essential features of the HSE-protocol to existing QKD protocols: the original quantum key distribution protocol of Bennett and Brassard [5] is referred to as BB84; the generalisation of BB84 to a protocol that uses c mutually unbiased bases and d-dimensional quantum systems [12] is called BKB01; the case where three MU bases are used in dimension two corresponds to the six-state protocol (6-state) [24, 32]; the protocol presented in Sec. 2 is denoted HSE (which stands for *highly sensitive to eavesdropping*); the case where only two bases are used corresponding to the protocol of Khan et al. (KMB09) [10]. Throughout the table, we assume that the HSE-protocol is applied to a set of c mutually unbiased bases. The pair of numbers, (d, c), in the second column correspond to the dimension of the quantum systems used in the protocol and the number of elements in

Protocol	(d,c)	$\mathcal{R}_{QB}$	$\mathcal{R}_{IT}$	$\mathcal{R}_t$	N_s
BB84	$(2,2)$	25.0%	n/a	50.0%	2.0
KMB09	$(2,2)$	33.3%	25.5%	25.0%	4.0
BKB01 (6-state)	$(2,3)$	33.3%	n/a	33.3%	3.0
HSE	$(2,3)$	57.1%	33.3%	13.2%	15.1
BKB01	$(3,2)$	33.3%	n/a	79.2%	1.3
KMB09	$(3,2)$	33.3%	33.3%	33.3%	3.0
BKB01	$(3,4)$	50.0%	n/a	39.6%	2.5
HSE	$(3,4)$	69.2%	50.0%	14.8%	20.3
BKB01	$(7,2)$	42.9%	n/a	140.4%	0.7
KMB09	$(7,2)$	33.3%	42.9%	42.9%	2.3
BKB01	$(7,8)$	75.0%	n/a	35.1%	2.8
HSE	$(7,8)$	86.0%	75.0%	12.7%	54.9

Table 1: Table comparing different QKD protocols in dimensions $d = 2, 3$ and 7; $\mathcal{R}_{QB}$ and $\mathcal{R}_{IT}$ are the quantum bit and index transmission error rates of an intercept-and-resend attack, respectively; $\mathcal{R}_t$ is the bit transmission rate defined in Eqn (3); finally, N_s is the average number of states Alice must send in order to share one bit with Bob. Note that the KMB09-protocol is a special case of the HSE-protocol.

the classical alphabet.

The third and forth columns of Table 1 show the QBER and the ITER respectively. The error rates, which have been calculated using Eqns. (14) and (15), show that by using $d+1$ MU bases, Alice and Bob can increase the QBER beyond that of BKB01. The fifth column displays the rate at which the two legitimate parties sharing one bit of information; that is $\mathcal{R}_s$ has been normalised so that it gives a *per bit* success rate[2]. The last column then shows the average number of states Alice needs to send in order to successfully share one bit of her key with Bob. This final column clearly demonstrates the trade-off between the error rate and the "cost" of producing a shared key. It is possible to make it easier to detect Eve but this comes at the expense of reducing the bit transmission rate.

At first sight, the protocol appears to have no special features relating to the dimension of the quantum systems used by Alice and Bob. However, an analysis of the optimal bases reveals that it is more efficient when the legitimate parties use systems of prime-power dimensions. In prime-power dimensions Alice and Bob can use constructions of $d+1$ mutually unbiased bases that are conjectured not to exist in composite dimensions such as $d = 6, 10, 12$, etc. In addition, in some dimensions, *inequivalent* sets of c MU bases are available. For example in dimension $d = 4$, there exits a three-parameter family of triples of MU bases [26, 38] or in dimension $d = 16$ there is a 17-parameter family of pairs of MU bases [39]. It may be that within these families there are some bases that

[2]Note that when the BKB01 protocol is applied to two MU bases in dimension $d = 7$, the rate at which bits are shared between Alice and Bob is larger than 100%. In this case, the legitimate parties use 7-dimensional quantum systems so that each time they are successful, they share an element of a 7 letter alphabet. Hence, the number of states Alice needs to send in order to share one *bit* is 0.7, i.e. less than one.

are experimentally more accessible than others. For example, Romero et al. [40] have considered a notion of inequivalent sets of MU bases involving the entanglement content of the bases and therefore, one aspect of the experimental difficulty in measuring and preparing systems in the corresponding bases.

If an experimenter finds that a particular measurement is easy to implement and that quantum systems prepared in the corresponding basis are readily available, they can use the HSE-protocol to distribute shared keys. Given the analytical form of the bases, we have shown how to calculate the error rate and the rate at which elements of a key are generated. Hence, to some extent, the protocol can be made to fit around experimental conditions, the question is then if the system noise enables an eavesdropper to disguise their presence. It may be that in practice it is better to search for measurements that can be performed efficiently in the laboratory (or in a purpose built device) than to find the analytical optimal bases.

In recent years, quantum physicists have realised that finite dimensional complex linear spaces are surprisingly rich both in physical content and from a mathematical perspective. This setting has led to many important physical discoveries and in particular, the ability to distribute keys in a secure way. In this paper, we have explored this mathematical structure further and found that, at least in principle, Alice and Bob can make it very hard for Eve to hide.

Acknowledgments

The author would like to thank Stefan Weigert, Tony Sudbery and Almut Beige for helpful comments on an earlier version of the manuscript.

References

[1] R. Rivest, A. Shamir and L. Adleman, *A method for obtaining digital signatures and public-key cryptosystems*, Comm. ACM **21**, 120 (1978).

[2] W. Diffie and M. Hellman, *New directions in Cryptography*, IEEE Trans. Info. Theory **22**, 644 (1976).

[3] M. Hellman, B. Diffie, and R. Merkle, *Cryptographic apparatus and method,* U.S. Patent #4200770 (1980).

[4] S. Wiesner, *Conjugate coding,* SIGACT News **15**, 78 (1983); originally written circa 1970.

[5] C. Bennett and G. Brassard, *Quantum Cryptography: Public key distribution and coin tossing*, Proc. of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, p. 175 (1984).

[6] A. Ekert, *Quantum cryptography based on Bell's theorem*, Phys. Rev. Lett. **67**, 661 (1991)

[7] S. Popescu and D. Rohrlich, *Nonlocality as an axiom for quantum theory,* Found. Phys. **24,** 379 (1994). arXiv:quant-ph/9508009.

[8] D. Mayers, *Unconditional security in Quantum Cryptography,* JACM **48,** 351 (2001). arXiv:quant-ph/9802025.

[9] P. Shor and J. Preskill, *Simple proof of security of the BB84 Quantum Key Distribution Protocol*, Phys. Rev. Lett. **85,** 441 (2000). arXiv:quant-ph/0003004.

[10] M. Khan, M. Murphy and A. Beige, *High error-rate quantum key distribution for long-distance communication,* New J. Phys. **11,** 063043 (2009). arXiv:0901.3909.

[11] V. Scarani, A. Acin, G. Ribordy and N. Gisin, *Quantum Cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations,* Phys. Rev. Lett **92**, 057901 (2004). arXiv:quant-ph/0211131.

[12] M. Bourennane, A. Karlsson and G. Björk, *Quantum key distribution using multilevel encoding*, Phys. Rev. A **64**, 012306 (2001).

[13] N. Cerf, M. Bourennane, A. Karlsson, and N. Gisin, *Security of quantum key distribution using d-level systems*, Phys. Rev. Lett. **88**, 127902 (2002). arXiv:quant-ph/0106049.

[14] A. Beige, B.-G. Englert, C. Kurtsiefer and H. Weinfurter, *Secure communication with single-photon two-qubit states*, J. Phys. A **35**, L407 (2002). arXiv:quant-ph/0101066.

[15] A. Beige, B.-G. Englert, C. Kurtsiefer and H. Weinfurter, *Secure communication with a publicly known key*, Acta Phys. Pol. A **101**, 357 (2002). arXiv:quant-ph/0111106.

[16] I. Bengtsson, W. Bruzda, Å. Ericsson, J-Å. Larsson, W. Tadej and K. Życzkowski, *Mubs and Hadamards of order six,* J. Math. Phys. **48**, 052106 (2007). arXiv:quant-ph/0610161.

[17] J. Schwinger, *Unitary operator bases*, Proc. Nat. Acad. Sci. U.S.A. **46**, 560 (1960).

[18] W. K. Wootters and B. D. Fields, *Optimal state-determination by mutually unbiased measurements*, Ann. Phys. **191**, 363 (1989)

[19] C. Bennett, G. Brassard, S. Breidbart and S. Wiesner, *Quantum Cryptography, or unforgeable subway tokens*, Advances in Cryptology: Proceedings of Crypto '82, Plenum, New York, pp. 267 (1982).

[20] C. Bennett, F. Bessette, G. Brassard, L. Salvail and J. Smolin, *Experimental Quantum Cryptography*, J. Cryptology **5**, 3 (1992).

[21] A. Ekert, B. Huttner, G. Palma, and A. Peres, *Eavesdropping on quantum-cryptographical systems*, Phys. Rev. A **50**, 1047 (1994).

[22] B. Huttner and A. Ekert, *Information gain in quantum eavesdropping*, J. Mod. Optics 41, 2455 (1994)

[23] C. Fuchs, N. Gisin, R. Griffiths, C.-S. Niu and A. Peres, *Optimal eavesdropping in Quantum Cryptography,* Phys. Rev. A **56**, 1163 (1997). arXiv:quant-ph/9701039.

[24] H. Bechmann-Pasquinucci and N. Gisin, *Incoherent and coherent eavesdropping in the 6-state protocol of Quantum Cryptography*, Phys. Rev. A **59**, 4238 (1999). arXiv:quant-ph/9807041.

[25] M. Bourennane, A. Karlsson, G. Björk, N. Gisin and N. Cerf, *Quantum key distribution using multilevel encoding: Security analysis*, J. Phys. A **35,** 10065 (2002). arXiv:quant-ph/0106049.

[26] S. Brierley, S. Weigert and I. Bengtsson, *All mutually unbiased bases in dimensions two to five,* unpublished (2009). arXiv:0907.4097.

[27] P. Butterley and W. Hall, *Numerical evidence for the maximum number of mutually unbiased bases in dimension six,* Phys. Lett. A **369**, 5 (2007). arXiv:quant-ph/0701122.

[28] S. Brierley and S. Weigert, *Maximal sets of mutually unbiased quantum states in dimension six,* Phys. Rev. A **78**, 042312 (2008). arXiv:0808.1614.

[29] S. Brierley and S. Weigert, *Constructing mutually unbiased bases in dimension six,* Phys. Rev. A **79**, 052316 (2009). arXiv:0901.4051.

[30] P. Jaming, M. Matolcsi, P. Móra, F. Szöllősi and M. Weiner, *A generalized Pauli problem and an infinite family of MUB-triplets in dimension 6*, J. Phys. A **42,** 245305 (2009). arXiv:0902.0882.

[31] A. Klappenecker, M. Rötteler, I. Shparlinski and A. Winterhof, *On approximately symmetric informationally complete positive operator-valued measures and related systems of quantum states*, J. Math. Phys. **46**, 082104 (2005). quant-ph/0503239

[32] D. Bruß, *Optimal eavesdropping in Quantum Cryptography with six states,* Phys. Rev. Lett. **81**, 3018 (1998). arXiv:quant-ph/9805019.

[33] D. Enzer, P. Hadley, R. Hughes, C. Peterson and P. Kwiat, *Entangled-photon six-state quantum cryptography*, New J. Phys. **4,** 45 (2002).

[34] R. Adamson and A. Steinberg, *Improving quantum state estimation with mutually unbiased bases*, unpublished (2008). arXiv:0808.0944.

[35] M. Reck, A. Zeilinger, H. J. Bernstein and P. Bertani, *Experimental realization of any discrete unitary operator,* Phys. Rev. Lett. **73**, 58 (1994).

[36] M. Żukowski, A. Zeilinger, and M. Horne, *Realizable higher-dimensional two-particle entanglements via multiport beam splitters*, Phys. Rev. A **55**, 2564 (1997).

[37] Y. Lim and A. Beige, *Multiphoton entanglement through a Bell multiport beam splitter*, Phys. Rev. A **71**, 062311 (2005). arXiv:quant-ph/0406047.

[38] G. Zauner, *Quantendesigns. Grundzüge einer nichtkommutativen Designtheorie*. PhD thesis, University of Wien, 1999.

[39] W. Tadej and K. Życzkowski, *A concise guide to complex Hadamard matrices,* Open Sys. Info. Dynamics **13**, 133 (2006). arXiv:quant-ph/0512154.

[40] J. Romero, G. Björk, A. Klimov, and L. Sánchez-Soto, *Structure of the sets of mutually unbiased bases for N qubits,* Phys. Rev. A **72**, 062310 (2005). arXiv:quant-ph/0508129.